Questions de certification, signature et cryptographie

Davio, Etienne

Published in:
Internet face au droit

Publication date:
1997

Document Version
le PDF de l'éditeur

Chapitre 2 - Questions de certification, signature et cryptographie

Etienne DAVIO*

* Assistant à la Faculté de droit de Namur, attaché de recherches au C.R.I.D.

I. Introduction - Internet, le mot est magique

Il ne se passe pas un jour sans que l'on s'interroge sur l'aptitude d'un média comme Internet à être un support propice à la formation de contrats. Il est certain que notre système juridique ne s'était pas préparé à l'émergence de cet univers virtuel à l'intérieur duquel les sujets de droit peuvent modeler les apparitions de leur être juridique sous la forme d'ectoplasmes insaisissables. A bien y regarder, la tentation est grande de pousser plus avant le parallélisme avec les sciences occultes.

Notre démarche sera celle de l'alchimiste. Le coeur de notre recherche concernera l'identification du cocontractant dans le commerce électronique.

Dans un premier titre, nous nous tournerons vers d'anciens grimoires pour bien comprendre la genèse d'un signe de première importance : il s'agit de la signature. Quelle place occupe-t-elle dans notre système juridique. Quel en est l'enjeu ?

Dans un deuxième titre, nous traiterons des incertitudes, du doute qui caractérise un nouvel élément, le réseau ouvert. Quel est ce cinquième élément qui semble se jouer de la terre, de l'eau, de l'air et du feu ? Comment ce lieu peut-il se révéler propice aux échanges contraignants ?

Nous aborderons dans notre troisième titre la question centrale de l'identification du cocontractant dans le réseau Internet. Un véritable parcours initiatique semble nécessaire pour faire son entrée sur les réseaux. L'acteur doit s'en remettre à la sagesse des autorités de certification. Nous envisagerons les lois qui gouvernent ces créateurs de certitude auxquels la cryptographie tient lieu de pierre philosophale. La cryptographie apparaît, en effet, seule capable d'assurer la transmutation de ce réseau, ces morceaux de métal mis bout à bout, en autoroute du succès pavée d'or.

II. La signature, objet singulier

II.1. La signature manuscrite : genèse d'un signe

La signature manuscrite que nous connaissons « est le vestige d'un véritable système de signes d'identité dont elle se détache au XVIème siècle ».[172] En synthétisant le propos de Madame Fraenkel, on peut retenir : primo, que les signes d'identité indiquent les caractéristiques d'un individu de sorte qu'on puisse le reconnaître, secundo, que le choix d'un système de signes d'identité est révélateur de la conception sociale que l'on se fait de l'identité d'un individu[173].

Il est intéressant de noter la place originale qu'occupe la signature manuscrite à côté des sceaux anciens, mais aussi des signes d'identité les plus modernes. Les signes de l'identité jusqu'au XVIème siècle, c'est-à-dire avant l'avènement de la signature manuscrite, privilégient la part intersubjective du soi, les déterminations de l'individu par le réseau de ses appartenances. Les signes dont s'entoure l'homme médiéval montrent le groupe auquel il appartient, quelle est sa place et son rang.[174]

La signature manuscrite rompt avec ces méthodes. La singularité de l'être est inscrite dans le signe, il y a personnalisation du signe. Le passage, au XVIème siècle, d'un système de sceaux à la signature manuscrite exprime l'apparition d'une nouvelle conception de l'identité. On abandonne une vision exotérique du soi, où l'individu est identifié au regard de ses liens aux autres, au profit d'une vision ésotérique du soi, où l'individu est identifié sur base de traits personnels irréductibles.

L'identification dans les réseaux électroniques se rapproche nettement du système médiéval d'identification en ce qu'il se réfère à des caractéristiques extérieures à l'individu dont attestent des tiers. Le débat sur la signature électronique se démarque nettement des idées arrêtées en matière de signature manuscrite. La perte du lien physique à la personne qui avait permis à la signature manuscrite de supplanter les autres signes d'identité est une donnée majeure. S'agit-il à nouveau d'une évolution dans la conception que l'on se fait de l'identité ou simplement cela tient-il aux caractères spécifiques des signes permettant l'identification, à savoir des numéros. A ce stade, nous ne pouvons rejeter catégoriquement l'idée d'une évolution de la représentation même que l'on se fait de l'individu. Il

172 B. FRAENKEL, *La signature. Genèse d'un signe*, Paris, Gallimard, 1992, p. 7.
173 B. FRAENKEL, *op. cit.*, p. 8.
174 B. FRAENKEL, *op. cit.*, pp. 10-11.

y a matière à réflexion sur le thème de l'identité de l'individu du fait du développement des réseaux[175].

II.2. L'empire de la signature manuscrite

II.2.1. Les fonctions de la signature

La signature a une double fonction.

Elle permet l'identification de l'auteur de l'acte. En ce sens, « la signature confère à l'acte son 'authenticité', 'la seule garantie de son origine'[176], puisqu'elle contient en elle-même la preuve intrinsèque qu'elle est l'oeuvre du scripteur, sans qu'il soit nécessaire d'avoir recours à la preuve testimoniale »[177]. La signature permet dès lors d'établir la présence physique du scripteur à l'acte.

Elle exprime la volonté du signataire : en apposant sa signature au pied de l'acte, il exprime sa volonté de s'en approprier le contenu. « La signature apparaît comme l'extériorisation d'une volonté interne. »[178]

II.2.2. La signature : définition en droit

Le concept de signature est indissociable des fonctionnalités recherchées. Ce faisant, notre système juridique a arrêté une définition de la signature de sorte que la notion apparaît figée dans sa forme et dans son contenu.

1° La signature doit être manuscrite. « Elle implique un mouvement corporel (de la main en principe), et elle ne peut être remplacée par la reproduction au moyen d'un timbre humide, par une griffe ou par un cachet »[179]. Sous la pression du monde des affaires, le législateur français a admis, de manière limitée, l'emploi de procédés non manuscrits pour apposer certaines signatures sur les effets de commerces et le chèque[180]. Le recours à de tels textes laisse penser que dans l'esprit du législateur[181] seule une signature manuelle peut être admise[182].

2° La signature doit consister dans l'apposition autographe de son nom[183]. Il convient à ce stade de s'entendre sur le concept de nom du signataire. La Cour de cassation belge considère que la signature est la marque manuscrite par laquelle le testateur révèle habituellement sa personnalité aux tiers[184]. La solution de la Cour de cassation française consiste à considérer qu'une signature, manuscrite s'entend, est valable dès qu'elle permet d'établir l'identité de l'auteur de l'acte et son adhésion au texte[185].

II.2.3. Les finalités juridiques de la signature

Où trouve-t-on trace de la signature dans le débat juridique ?

Le plus souvent « l'acte signé, le titre, est exigé *ad probationem*, en vue d'établir l'existence de l'acte juridique que l'on invoque »[186]. En pareil cas, les vices entourant l'*instrumentum* vont désavantager le plaideur sur le plan probatoire, sans que la validité du *negotium* ne soit remise en question.

« Mais parfois l'acte est requis *ad validitatem*, l'écrit et la signature étant indispensable pour l'existence juridique de l'acte lui-même. L'absence de signature entraîne alors la nullité du negotium »[187].

« S'il est vrai que les contrats se forment *solo consensu*, il n'en reste pas moins que, d'un point de vue sociologique et pratique, *idem est non esse et non probari* »[188]. «L'on ne sait plus très bien s'il faut dire 'je signe parce que je veux', ou 'je veux parce que je signe' »[189].

Nous aurons à revenir sur les différents enjeux de la signature. Le débat sur la signature électronique, de par son ampleur, laisse penser que les finalités sont appelées à changer.

175 « Ainsi, dans la mesure où la place de l'individu en société s'établit non exclusivement par la participation à des actes de proximité (mis en oeuvre par la comparution des personnes) mais, de plus en plus, par des échanges télématiques, au cours desquels la personne s'identifie par numéro, on peut sans risque admettre que la réalité sociale de l'individu ne se limite pas aux situations retenues pour servir de critère à l'état civil et qu'elle est en pleine évolution. La logique dicterait qu'à la nature nouvelle de la situation de l'homme en société corresponde une définition nouvelle de son état civil » E. DUBUISSON, *La numérotation des personnes physiques*, thèse de doctorat, Université de Paris II, 1994, p. 143.

176 H. DE PAGE, t. III, n° 777, B.

177 M. VAN QUICKENBORNE, « Quelques réflexions sur la signature des actes sous seing privé », note sous Cass., 28 juin 1985, *R. C. J. B.*, 1985, p. 68. Il faut néanmoins garder à l'esprit la faculté de dénégation d'écriture (article 1323 du Code civil).

178 M. VAN QUICKENBORNE, *op. cit.*, p. 69.

179 N. VERHEYDEN-JEANMART, *Droit de la preuve*, Précis de la Faculté de Droit de l'UCL, Bruxelles, Larcier, 1991, p. 238.

180 Loi du 6 juin 1966, citée par M. VAN QUICKENBORNE, *op. cit*, pp. 87-88.

181 Une situation comparable peut être observée en Belgique. Sur cette question voy M. VAN QUICKENBORNE, *op. cit.*, p. 88.

182 Contra D. SYX, « Vers de nouvelles formes de signature. Le problème de la signature dans les rapports électroniques », *Droit de l'informatique*, 1986, p. 136, qui observe cette exigence en jurisprudence, mais dénie l'attachement du législateur à la forme manuscrite de la signature.

183 M. VAN QUICKENBORNE, *op. cit.*, p. 71-74 et les références citées.

184 Cass. 7 janv. 1955, *Pas.*, p. 456; Cass. 2 oct. 1964, *Pas.* 1965, p. 106.

185 Cass. fr., 24 juin 1952, *Sem. jurid.*, 1952, 7179.

186 M. VAN QUICKENBORNE, *op. cit.*, p. 67.

187 M. VAN QUICKENBORNE, *op. cit.*, p. 67.

188 M. VAN QUICKENBORNE, *op. cit.*, p. 70.

189 J. CARBONNIER, *Droit civil*, coll. Thémis, II, n° 99, p. 339, cité par M. VAN QUICKENBORNE, *op. cit.*, p. 70.

II.3. La signature et le numéro

II.3.1. La numérotation des personnes physiques

Sous ce titre, Etienne Dubuisson s'est intéressé aux rapports sans cesse plus étroits entre la personne et le nombre.[190]

A la base de toute opération d'identification des personnes physiques, il y a la détermination des éléments sur base desquels on vérifiera l'identité. Classiquement, ces éléments sont ceux de l'état civil : nom, domicile...[191] S'interrogeant sur le rôle croissant joué par le numéro dans l'identification des personnes, monsieur Dubuisson constate que le numéro intervient là où les méthodes d'identification par les éléments de l'état sont dépassées tant du fait des lourdeurs de gestion qu'elles occasionnent (mémorisation de la diversité des éléments de l'état) que par l'impossibilité d'en intégrer la preuve (absence de comparution de la personne, irrecevabilité de la signature manuscrite).[192]

L'efficacité de l'identification par le numéro est très grande. « Elle présente en effet une possibilité de fonctionnement total : elle saisit l'irréductibilité individuelle de même qu'elle intègre l'expansion croissante du groupe. Elle combine les deux grandeurs de l'identité : l'attachement au groupe et la singularité au sein du groupe, ce qui est la fonction propre de tout système social d'identification »[193].

Le numéro sert à l'individualisation des personnes par l'utilisation d'un substrat abstrait non corporel. L'idée de présentation corporelle n'est plus ici opérante.[194] Toute adéquation qu'il y ait entre la personne et le numéro, elle n'est pas absolue parce qu'elle est médiate. Elle n'existe que par la lecture qu'en fait l'agent agissant comme décodeur. Notamment, l'individu dans un travail réflexif sur lui-même, en faisant abstraction du décodeur, ne se reconnaîtra pas dans le numéro, tout simplement parce qu'à raison de cette abstraction, le numéro ne signifie plus rien[195].

L'aspect personnel de l'identification, présent dans le système du nom, est absent.[196]

190 E. DUBUISSON, *La numérotation des personnes physiques*, Thèse de doctorat, Université de Paris II, 1994.

191 A cette étape fera suite l'individualisation qui consiste à reporter les critères retenus sur un individu particulier.

192 E. DUBUISSON, *op. cit.*, p. 143.

193 E. DUBUISSON, *op. cit.*, p. 21.

194 E. DUBUISSON, *op. cit.*, p. 47.

195 E. DUBUISSON, *op. cit.*, p. 98.

196 L'impersonnalité des numéros semble structurelle et donc indépassable. L'état civil définit, en effet, l'individu dans une position spatio-temporelle, c'est à dire par un quadrillage; en un temps et un lieu ne peut se trouver qu'une personne; l'individu pourra ainsi prendre conscience, en même temps que de ses déterminations naturelles, de son opposition aux autres et donc de son identité. Dans la numérotation, il s'agit plutôt de calibrage dont la notion s'oppose à celle de quadrillage : elle définit une situation d'appartenance à un ensemble d'éléments ressemblant à un modèle. E. DUBUISSON, *op. cit.*, p. 98.

L'individu, ignorant de sa position, dans cette classification qualitative, ne peut pas se positionner par rapport aux autres individus; son numéro ne lui permet pas de se reconnaître.

L'absence de ce sentiment pour l'individu qui ne se reconnaît pas dans le numéro constitue le point névralgique des réseaux télématiques par carte; en effet, malgré l'ingéniosité des systèmes créés, on n'est jamais sûr que la personne qui utilise le terminal au moyen de sa carte est bien le porteur légitime. C'est le problème de l'identification au sens télématique du terme : « L'identification consiste à s'assurer que le porteur de la carte en est effectivement le porteur légitime. Il doit le prouver à la carte par la connaissance d'un code secret ». S'y adjoint la nécessité de vérifier que la carte utilisée n'est pas fausse, c'est la problème de l'authentification : « Sachant que l'utilisateur a été identifié comme propriétaire légitime de sa carte, il reste à la carte à prouver son authenticité au système informatique »[197]

Les vertus de la numérotation des personnes comme outil d'identification reposent toutes entières sur la préservation du lien artificiel entre la personne et son numéro. Dans la suite, nous concentrerons notre attention sur l'utilisation du numéro aux fins de signature. Tout doit être fait pour qu'au niveau de l'attribution, de la réception et de l'utilisation, l'intimité et la confidentialité du lien puissent être préservées.

II.3.2. La signature électronique : acte premier

De longue date, la technique informatique offre les moyens d'identifier, avec plus au moins de certitude, l'auteur d'un message déterminé. On a très tôt moment fait référence aux signatures électroniques.

Les premières applications du genre apparaissent dans les relations triangulaires entre le commerçant, le titulaire et l'émetteur de la carte (terminal point de vente), ainsi que dans le cas des distributeurs automatiques de billets. A ce stade, nous nous situons dans ce qu'il est convenu d'appeler les réseaux fermés. Une préoccupation centrale apparaît alors : assurer que celui qui utilise le moyen de paiement électronique ne puisse se soustraire aux obligations qui en résultent. « La reconnaissance de la signature informatique est une nécessité impérieuse pour garantir le paie-

197 J. LARRIEU, *Une société sans papier, Notes et documents*, La documentation française, N° 4914-4915, p. 211, cité par E. DUBUISSON, *op. cit.*, p. 99.

ment par carte. »[198] On observe alors une adaptation réciproque de la technique et du droit[199].

A ce stade, nous sommes encore très loin de la notion de signature électronique telle qu'elle se développe aujourd'hui. Rétrospectivement, ces mécanismes s'en distinguent dans la mesure où les cartes et codes d'accès constituent bien plus des mécanismes d'autorisation d'accès dans des systèmes fermés en vue d'opérations prédéfinies[200].

D'un point de vue méthodologique, la reconnaissance à ces techniques d'authentification d'une valeur juridique comparable à la signature manuscrite peut prendre trois orientations.

La première démarche est interprétative. Se fondant sur une analyse fonctionnelle de la notion de signature, certains auteurs soutiennent que dès à présent les cours et tribunaux peuvent reconnaître la même valeur aux signatures électroniques que celle reconnue à la signature manuscrite, pour autant que les fonctionnalités d'identification de l'auteur et d'adhésion au contenu soient rencontrées[201].

La deuxième approche est contractuelle. Elle consiste pour les contractants à s'entendre sur la forme et la valeur reconnues aux signatures électroniques et de convenir, par exemple, de leur assimilation à des signatures manuscrites. La validité de ces conventions est parfaitement admise. De telles clauses figurent de longue date dans les contrats de banque à distance. La généralisation de ces clauses a pour effet de couper court aux développements jurisprudentiels.

98 M. BOIZARD, « Preuve des paiements par cartes bancaires et signature informatique », *Cahier Lamy Droit de l'informatique*, E, 1988, p. 8.

99 A cette époque on constate que le droit est quelquefois en avance sur la technique, en admettant des techniques de « signature » quelque peu imparfaites. On peut illustrer ce phénomène par un exemple : le moment de l'apposition de la signature électronique. Les premiers systèmes de retrait d'argent à l'aide d'une carte invitaient le titulaire de la carte à composer, dès le début, le numéro de code secret et de déterminer, ensuite, le nombre de billets souhaités. Ainsi ce code combiné à la présentation de la carte constituait la signature d'un acte à venir. Cherchant à voir là une signature valide de l'acte, J. Larrieu affirme que la jurisprudence se montre assez indifférente à la place de la signature manuscrite, que l'on s'attend pour le reste à trouver en bas de l'acte (J. LARRIEU, « Les nouveaux moyens de preuve : pour ou contre l'identification des documents informatiques à des écrits sous seing privé? », *Cahiers Lamy droit de l'informatique*, J/88, p. 29, n° 50). Le parallèle établi entre le moment et la place de la signature manuscrite ne semble pas pouvoir être reproduit dans le contexte de la signature informatique. Si l'on s'attend à trouver la signature au bas de l'acte, c'est parce qu'elle marque son achèvement et l'adhésion du signataire au contenu de l'acte. La jurisprudence a certes admis qu'une signature placée ailleurs dans le texte puisse avoir le même effet, l'idée sous-jacente étant tout de même que cette signature intervienne après la rédaction de l'écrit (hormis l'hypothèse du blanc-seing) et qu'elle couvre l'ensemble de l'acte (N. VERHEYDEN-JEANMART, *op. cit.*, p. 240). L'assimilation de l'accès au système avec la signature d'un acte non encore rédigé est problématique. L'évolution technique a tenu compte de ce problème en implémentant deux opérations distinctes, l'accès d'un utilisateur à un réseau par le moyen d'une identification et l'authentification de actes juridiques passés par un procédé de signature électronique. Faut-il en conclure que les actes passés dans de telles circonstance n'étaient pas signés ? L'évolution des techniques laisse apparaître qu'il s'agissait là d'une signature en mode mineur...

200 S. PARISIEN, P. TRUDEL, *L'identification et la certification dans le commerce électronique*, Université de Montréal, Faculté de Droit, Avril 1996, p. 132.

201 D. SYX, *op. cit.*, p. 134 et s.

La troisième orientation possible est la voie législative.

— Soit que l'on définisse largement le concept de signature de façon à pouvoir y inclure des formes électroniques de signature. En ce sens, l'article 2827 du Code civil du Québec qui donne le définition suivante : « la signature consiste dans l'apposition qu'une personne fait sur un acte de son nom ou d'une marque qui lui est personnelle et qu'elle utilise de façon courante, pour manifester son consentement ». « Du fait de cette formulation large, rien dans les termes de l'article 2827 ne s'oppose à l'utilisation de signatures dites électroniques. Il apparaît en effet légitime de soutenir qu'une signature électronique constitue bel et bien une marque dont le caractère personnel se trouve par ailleurs assuré par le haut niveau de confidentialité qui entoure généralement les mécanismes de signature électronique »[202].
— Soit que l'on définisse clairement ce qu'il faut entendre par signature électronique et que l'on fixe la valeur de cette signature[203].

En conclusion, tant sous l'angle technique que juridique, les techniques fiables de signature électronique sont à portée de main, du moins dans les réseaux fermés. S'agissant de conclure des contrats sur des réseaux ouverts, c'est l'absence de véritable code d'identification pouvant être qualifié de « signature électronique » qui va poser problème[204]. Pour résoudre ce délicat problème, on aura recours aux infrastructures à clés publiques.

202 S. PARISIEN, « Aspects juridiques et technologiques des mécanismes de signature électronique : une analyse comparative », in actes du Colloque *Faire des affaires en toute sécurité sur les autoroutes de l'information*, 10 novembre 1995, http://www.droit.umontreal.ca/AQDIJ/Colloque_10_11_95/Parisien/parisien_udm.html, p. 4.

203 Cette voie a été suivie dans le Utah Digital Signature Act publié dans l'EDI Law Review, 1995, 2, 157-196.

204 J. -P. BUYLE, O. POELMANS, « Internet : quelques aspects juridiques », *D.I.T.*, 1996/2, p. 13.

III. La sécurité dans les réseaux ouverts

III.1. Définition du réseau ouvert

Les réflexions juridiques, déjà anciennes, relatives à la formation des contrats par des moyens électroniques[205] semblent devoir être relues en considération d'un contexte nouveau : celui de la communication sur les réseaux ouverts.

En quoi un réseau ouvert se différencie-t-il d'un réseau fermé[206] ? A bien y regarder les critères de distinction varient.

Le critère premier de distinction se fonde sur le fonctionnement technique du réseau et, en particulier, sur la nature des contrôles exercés par les entités chargées d'administrer le réseau.

Ainsi, H. Perrit définit un système fermé comme un système dans lequel tout le contenu, les interfaces de communication, le stockage d'information, la réalisation de software et la sécurité est contrôlée par une entité unique : une société gérant un réseau local[207] ou un babillard électronique[208]. En présence d'un tel réseau, l'opérateur du système peut contrôler la population des utilisateurs[209].

Par opposition, un système ouvert est un système dans lequel aucune entité administrative ou légale ne contrôle les activités de communication, le stockage d'information ou les utilisateurs.

Le réseau des réseaux, Internet, répond parfaitement à cette idée. « La structure décentralisée de l'Internet, à l'origine conçue pour résister à toute tentative de destruction exclut virtuellement toute possibilité de contrôle par une autorité unique qui prétendrait exercer la maîtrise du réseau »[210]. L'absence de contrôle centralisé (et, qui plus est, son impossibilité radicale), constitue certainement une donnée majeure pour le juriste.

Un second critère retenu consiste à désigner l'environnement ouvert comme un environnement « où plusieurs intervenants étrangers et inconnus l'un à l'autre peuvent jouer »[211]. Cette caractéristique est intimement liée à la configuration technique des réseaux. Il faut cependant constater que cette caractéristique n'est pas exclusive à la communication au travers des réseaux ouverts. Ce qui, par contre, semble caractéristique des réseaux ouverts, c'est que, d'emblée, des internautes, qui ne se connaissent pas, souhaitent entrer en relation contractuelle dans un contexte électronique. A l'opposé « l'EDI sur les réseaux fermés présuppose une relation commerciale préexistante qui donne lieu à la possibilité d'encadrer les transactions par une convention entre les intervenants »[212].

L'absence de prise de connaissance préalable hors réseau et dès lors l'impossibilité d'asseoir les relations électroniques dans un cadre papier apparaît tant comme une évidente nécessité pour les praticiens des réseaux que comme un défi à nos systèmes juridiques.

III.2. La sécurité en droit

Tout réseau, pour être support à la transaction, a besoin d'un certain niveau de sécurité. En fait, il ne peut être question de transactions commerciales dans un réseau ouvert qui ne se serait pas donné les moyens de sécurité pour gérer les risques inhérents à son ouverture[213].

A ces risques correspondent des réponses techniques[214], lesquelles ne peuvent trouver leur pleine mesure que si elles sont couplées à une véritable sécurité juridique.

205 B. AMORY, M. SCHAUSS, « La formation de contrats par des moyens électroniques », *Droit de l'informatique*, 1987/4, pp. 206-215.

206 S'agissant de définir les réseaux, on peut identifier deux composantes. D'une part, la composante physique, c'est-à-dire les raccordements entre les différents terminaux de tous ceux qui souhaitent entrer en communication. D'autre part, la composante intentionnelle : le réseau est une réunion de personnes. Dans cette ligne, le réseau apparaît comme l'ensemble des usagers interconnectés. Sur cette question voy. P. TRUDEL, « Introduction au droit du commerce électronique sur l'Internet », *Revue du Barreau (Canada)*, 1995, pp. 521-551 citant A. S. HAMMOND, « Private Networks, Public Speech : Constitutional Speech Dimension of Access to Private Networks », [1994] 55, *University of Pittsburg Law Review*, 1085, 1095.

207 L. A. N. : local area network.

208 B. B. S. : bulletin board services.

209 H. PERRIT, « Security in open networks : maintaining confidentiality and getting paid », http://ming. law.vill.edu/chron/articles/pbisecu6.htm.

210 P. TRUDEL, *op. cit.*, pp. 521-551, qui constate que, dans le contexte des réseaux ouverts, les possibilités effectives de contrôle sont aux mains de ceux qui administrent les différents sites entre lesquels des interconnexions existent ou sont possibles.

211 Y. POULLET, « Les transactions commerciales et industrielles par voie électronique. De quelques réflexions autour du droit de la preuve », in *Le droit des affaires en évolution. Le juriste face à l'invasion informatique*. Colloque ABJE, 24 octobre 1996, Bruxelles, Bruylant, Anvers, Kluwer, 1996, p. 48.

212 D. G. MASSE, « L'autoroute de l'information : convergence du droit et de la technologie », in actes du Colloque *Faire des affaires en toute sécurité sur les autoroutes de l'information*, 10 novembre 1995, http://www.droit.umontreal.ca/A...loque_10_11_95/Masse/aqd95.html, p. 7.

213 D. G. MASSE, *op. cit.*, p. 6 qui constate « qu'afin d'être propice au commerce, une forme de communication doit fournir un moyen, jugé acceptable par la communauté commerciale, d'assurer que la certitude soit suffisante pour justifier le risque d'y transiger ».

214 J. HUBIN, *La sécurité informatique*, Cahier du Crid, n° 13, à paraître, Bruxelles, Story Scientia, 1996 qui définit la sécurité informatique comme la gestion des techniques physiques, logiques et humaines destinées à protéger, contre les accidents, les erreurs et les comportements malicieux, les êtres humains qui confient certaines valeurs à des systèmes informatiques fonctionnant dans un certain environnement.

D'un point de vue juridique, la notion de sécurité se réfère, essentiellement, à la possibilité 1° d'authentifier l'utilisateur du système tant pour éviter les usurpations d'identité que pour assurer la non-répudiation d'une volonté exprimée; 2° d'assurer l'intégrité du message tant à l'égard de modifications accidentelles que malveillantes; 3° de garder des traces de la transaction pour valoir preuve[215]. Plus généralement, il s'agit de permettre l'expression véritable du consentement.

Nous arrivons ici à un moment charnière. A ce stade, nous devons insister sur ce qui nous apparaît comme la caractéristique la plus marquante du réseau ouvert. Dans un tel système, la sécurité est contenue à même le message par le moyen des procédés de signature électronique[216]. Désormais, la sécurité d'un réseau réside non pas dans sa structure, mais dans la sécurisation du flux d'information. Chaque information, chaque message va être sécurisé par sa signature électronique.

C'est ici qu'éclate au grand jour le rôle capital que doivent jouer les mécanismes de signature électronique. Ils leur revient d'assurer la sécurité de l'échange.

Fondamentalement le débat sur la signature est un débat sur la sécurité de l'échange des consentements.

III.3. La sécurité comme condition de validité des contrats

La question que l'on doit se poser est la suivante : dans un réseau ouvert, peut-on valablement exprimer son consentement sans signature électronique ? Et de se demander si au-delà de la simple preuve de la volonté exprimée, la présence d'une signature électronique ne participe pas de la validité du consentement.

De façon générale, « il serait..., erroné de ramener le problème de la signature à un simple problème de preuve. La valeur de preuve de la signature n'apparaîtra en général que dans un stade ultérieur, lorsque surgit un différend entre les parties ou si l'un ou l'autre tiers veut vérifier l'identité des parties et le contenu de leur convention. Au moment même de l'acte juridique ou lors de sa fixation par écrit ou sous une autre forme, simultanément ou peu après, la fonction d'identification et de confirmation de la signature prévaudra : les parties se donnent un signe qui manifeste

215 B. AMORY, M. SCHAUSS, « La formation des contrats par des moyens électroniques », *Droit de l'informatique*, 1987/4, p. 207.

216 « Les principales garanties de sécurité quant à l'identification de l'émetteur, à l'intégrité des messages et quant à leur confidentialité résident non pas dans la structure du réseau lui-même, mais bien dans la sécurisation des messages qui y sont véhiculés » S. PARISIEN, P. TRUDEL, *op. cit.*, p. 27.

cette double fonction d'une manière suffisamment fiable et sûre. La signature possède dès lors une importante valeur de sécurité »[217].

A la réflexion le détour par le moyen-âge n'était pas inutile. Depuis son origine la signature apparaît comme un signe de validation[218]. Un récent article de Monsieur Wilms nous enseigne que la signature doit être vue comme une subsistance des rituels qui, par le passé, entouraient la naissance des contrats[219].

Ce qui a permis de cantonner la signature manuscrite dans le champ probatoire, c'est le fait de la maîtrise préalable de l'environnement. Il importe de constater que la fonction d'identification reconnue à la signature manuscrite est réduite. « Dans le cadre contractuel courant, malgré le fait que nous attachons beaucoup d'importance à la signature..., la signature n'est guère le moyen le plus important, ni même l'élément déterminant dans l'identification du cocontractant »[220]. Cet auteur constate, en effet, que dans les rapports contractuels traditionnels, l'identité des parties est établie par un ensemble de facteurs : la connaissance physique que les parties ont l'une de l'autre, composée du sexe, de la physionomie et des caractéristiques de la voix de la personne; la renommée de la personne et son introduction par des personnes que nous considérons fiables; la reconnaissance sur base de documents émis par des autorités fiables...[221].

Dans un réseau ouvert, la signature électronique est appelée à jouer seule la fonction d'identification d'un partenaire, laquelle doit avoir lieu en amont du contrat. La signature électronique apparaît comme un processus incontournable afin de permettre l'expression du consentement d'une personne particulière. Cette vision dynamique de la signature nous amène à conclure qu'elle participe directement à l'expression du consentement et donc à la formation du contrat.

Il est en tout cas du ressort des parties de ramener l'exigence de signature dans le domaine de la formation du contrat et de convenir que l'échange contraignant ne peut résulter que d'expressions de la volonté signées électroniquement. De fait, la chose est courante; de nombreuses transactions sur les réseaux ne pourront arriver à leur terme à défaut pour une partie d'avoir suivi correctement le processus de signature. La tendance généralisée au contrôle systématique des signatures électroniques conforte cette approche.

217 D. SYX, *op. cit.*, p. 136.

218 B. FRAENKEL, *op. cit.*, p. 19.

219 W. WILMS, « Van handtekening naar elektronische notaris-De validering van elektronische communicatie », *R. W.*, 1995-1996, p. 839.

220 D. G. MASSE, *op. cit.*, pp 10 et 11.

221 On peut tenir un raisonnement assez semblable dans l'hypothèse d'une communication en réseau fermé, la configuration du réseau, la connaissance préalable qu'ont les parties l'une de l'autre, les fins pour lesquelles la communication est établie vont participer, au côté des éléments de signature, à l'identification et à la reconnaissance du co-contractant.

IV. L'identification du contractant dans un réseau ouvert

IV.1. Le chiffrement aux fins de signature

IV.1.1. Position du problème

Nous abordons ici la problématique délicate de l'identification des acteurs, dans un environnement qui n'est soumis à aucun contrôle qui en limite l'accès.[222] A priori, le réseau ouvert n'offre aucune certitude sur l'identité d'un interlocuteur. Comment s'assurer que celui-ci est bien celui qu'il prétend être ?

A cette question, se rattache la question de savoir si le cocontractant a bel et bien manifesté sa volonté de s'approprier le contenu de l'acte.

Dans la recherche de procédés qui permettraient de s'assurer de l'expression du consentement d'une personne déterminée, les mécanismes de cryptographie, en particulier les procédés de cryptographie asymétrique vont apporter une aide déterminante.

D'autres procédés ont été mis en avant, il s'agit des procédés de signature biométrique, voire de nouveaux procédés cryptographiques. Le juriste doit y être attentif.

IV.1.2. La cryptographie à clé publique

On peut fermement affirmer qu'avec la cryptographie asymétrique, le 20ème siècle finissant a trouvé la pierre philosophale. Dans l'univers des réseaux, l'information qui transite d'un point à un autre en toute sécurité vaut de l'or. A ce jour, le juriste doit se réconcilier avec les chiffres et en reconnaître la magie.

La fonction première de la cryptographie vise à rendre secret le contenu d'une communication.

Ce résultat peut être atteint par les mécanismes de cryptographie classique, également appelée cryptographie symétrique, en raison de l'utilisation d'une clé identique pour chiffrer puis pour déchiffrer. L'expéditeur, utilise une clé secrète pour rendre illisible un message, le

222 D. G. MASSE, *op. cit.*, p. 5, qui pour sa part considère qu'Internet est un réseau ouvert, en ce sens « qu'il n'est soumis à aucun contrôle qui en limite l'accès ».

destinataire utilisera une clé secrète identique pour lire le message. La faille d'un tel système est la nécessité d'un partage de la clé secrète, laquelle doit exister en deux exemplaires.

La cryptographie moderne ou cryptographie asymétrique a résolu cette question du partage des clés.

La cryptographie asymétrique également appelée cryptographie à clé publique[223] consiste à déterminer, pour chaque utilisateur, deux clés de chiffrement reliées entre elles. Un message chiffré avec l'une des clés ne peut être déchiffré qu'avec l'autre et vice versa. La cryptographie est dite asymétrique parce la clé qui sert à chiffrer n'est pas la même que celle qui sert à déchiffrer. Le lien mathématique entre les deux clés est tel qu'il est impossible de découvrir une des clés en partant de l'autre.

Les deux clés liées vont connaître des sorts opposés. L'une est gardée secrète, connue de son seul titulaire, l'autre est rendue publique, c'est la clé publique.

La première fonction de la cryptographie asymétrique est de rendre un message illisible à tous sauf à son destinataire. Il s'agit d'assurer la confidentialité d'une communication. Pour ce faire, Bob, expéditeur du message, va le chiffrer avec la clé publique du destinataire, Alice. Dès ce moment, le message chiffré ne pourra plus être déchiffré qu'à l'aide de la clé secrète d'Alice. C'est à ce stade que surgit, le débat contemporain sur les éventuelles restrictions législatives à l'usage de la cryptographie.

La seconde fonction d'un tel système est une fonction de signature. Comment Bob peut-il convaincre Alice qu'il est bien l'auteur d'un message ? Si Bob, auteur d'un message chiffre celui-ci avec sa clé secrète (qu'il est, par définition, seul à connaître) et l'expédie à Alice, cette dernière va procéder au déchiffrement du message à l'aide de la clé publique de Bob. Si Alice parvient de la sorte à déchiffrer le message, elle acquiert la certitude que ce message provient bel et bien de Bob.

En résumé, si Bob veut rendre confidentiel le message qu'il destine à Alice, il le chiffre avec la clé publique d'Alice. S'il veut signer ce message, il le chiffre avec sa clé secrète. Et bien évidemment, il peut combiner les deux fonctions.

A ce stade, on peut identifier deux zones de risques, l'une a trait à la clé secrète, l'autre à la clé publique.

IV.1.3. Les risques afférents à la conservation de la clé secrète

On constate que les procédés de cryptographie asymétrique permettent une gestion efficace du risque informatique. Cela ne saurait nous faire

223 Dont l'apparition remonte à 1975.

oublier les risques physiques liés à la conservation de la clé secrète par son titulaire. En effet, si ce dernier perd la maîtrise de sa clé secrète, une tierce personne pourrait s'en servir et signer en lieu et place du titulaire de la clé.

De manière générale, le titulaire d'une clé secrète doit en assurer une conservation des plus attentives. En outre des mécanismes d'opposition et de révocation de clés existent dans tous les systèmes. Les responsabilités du titulaire quant à la conservation de sa clé secrète sont des plus lourdes. A cet égard, deux remarques doivent être formulées. *Primo*, la protection de cette relation singulière doit être assurée tant par une information de l'utilisateur que par la mise en place de mécanismes qui confortent le lien entre la clé secrète ou son support et son titulaire. En ce sens nous recommandons qu'une clé secrète soit systématiquement rapprochée de son titulaire par le recours à un code secret à mémoriser.

Secundo, l'apparente infaillibilité logique des systèmes conduit à reporter l'intégralité du risque sur le titulaire de la clé secrète. Cette situation est dénoncée par Benjamin Wright qui condamne la tendance à mettre tous les oeufs dans le même panier, à savoir la clé secrète.[224] Car, en effet, si par impossible un cryptosystème était cassé par un ingénieux fraudeur, le préjudice de l'utilisation de cette clé secrète forgée incomberait au titulaire de la clé secrète originale lequel est présumé avoir assuré incorrectement la conservation de sa clé secrète.

IV.2. Les Autorités de Certification

IV.2.1. Le certificat de clé publique

Si on se tourne vers la clé publique, une question se pose

224 Pour Benjamin Wright, la stratégie adoptée dans le *Utah Act* suppose un renversement de la charge de la preuve ainsi qu'une concentration du risque sur la clé secrète. (Cette vision est transposable à la plupart des solutions législatives ou conventionnelles qui mettent en place des infrastructures à clés publiques). « Not only does the Utah strategy shift risk to the private key, it concentrates the risk there. The *Utah Act* gives recipients like Bob strong reason to expect that if a document is signed with Alex's private key then Alex is legally responsible for the document. *Utah Act* section 46-3-401 provides that a document signed with a digital signature is normally presumed to be signed by the person owning the relevant private key (so long as his public key is certified by a licensed CA)... This presumption in turn gives Alex powerful incentive to protect the key... Under the Utah strategy, control of Alex's private key becomes all important. In other words, virtually all the eggs are placed in one basket- the private key », B. WRIGHT, « Eggs in baskets : Distributing the Risks of Electronic Signature », communication présentée à Montréal, le 31 août 1995 dans le cadre de la conférence *Faire des affaires en toute sécurité sur les autoroutes de l'information*, p. 4, cité par S. PARISIEN, « Aspects juridiques et technologiques des mécanismes de signature électronique : une analyse comparative », http://www.droit.umontreal.ca/AQDIJ/Colloque_10_11_95/Parisien/parisien_udm. html. Le texte de B. Wright est accessible, contre rémunération à l'adresse http://www.infohaus.com/access/by-seller/Benjamin_Wright/Benjamin_Wright. Eggs_in_Baskets.paid.txt.

Comment être certain que telle clé publique, présentée comme étant celle de Bob, est effectivement la sienne ?

L'utilisation de la cryptographie à clé publique aux fins de signature électronique suppose le recours à des mécanismes de contrôle visant à s'assurer que la clé rendue publique est bien celle de la personne qui s'en prétend titulaire. Un tel contrôle va être rendu possible grâce aux certificats de clés publiques qui émanent d'entités qui peuvent attester de l'existence d'un lien entre une clé publique et tel utilisateur déterminé.

Deux figures de contrôle peuvent être envisagées soit une structure de type pyramidal, soit une structure de type horizontal. Nous ne nous attarderons pas sur cette seconde forme de certification, quoique cette dernière est largement répandue, c'est en effet sur base du web-of-trust que sont certifiées les clés publiques générées dans le cadre du PGP[225]. Dans pareil cas il n'y a pas de hiérarchisation, on ne parle pas d'autorité. La certification est le fait de pairs.

> « Certification authorities are not the only means by which strangers can be persuaded to trust each other. An alternate system, called the web-of-trust, blurs the distinction between CAs and users. Every participant in a web-of-trust system is able to issue notices about whom they know and trust, and there is no central authority.
>
> The web-of-trust model has the advantage of being independent of any central authority. It has the disadvantage that it requires Alice either to trust strangers when she has no friends in common with Bob or to accept that there are large numbers of people with whom she cannot securely communicate. In contrast, the CA model is designed to make it possible for all strangers to communicate regardless of whether they have any friends in common, and to define with some precision the degree of trust that they can put in the CA's representations about strangers ».[226]

IV.2.2. Les missions de l'autorité de certification : délivrance et gestion des certificats

Les autorités de certification sont des tiers de confiance qui ont pour mission de renforcer la fiabilité et la sécurité des mécanismes de cryptographie à clé publique.[227] La notion d'autorité de certification est définie dans la norme X 509 de l'UIT comme étant « une autorité chargée par un

225 Voy. P. ZIMMERMANN, PGP User's Guide Volume I : Essential Topics (Oct. 11, 1994), accessible à l'adresse URL ftp://net-dist.mit.edu/pub/PGP.

226 M. FROOMKIN, « The essential role of trusted third parties in electronic commerce », 75 Gregon L. Rev. 49 (1996), disponible à l'adresse http://www.law.miami.edu/~froomkin/articles/trusted.htm.

227 UIT-T, Recommandation X. 509, Annuaire- cadre d'authentification, note 323, art. 3.3 c). D'autres tâches de certification peuvent encore être accomplies par l'autorité de certification. Ainsi elle peut certifier des caractéristiques de la personne autre que l'identité : âge, appartenance à un ordre professionnel, lieu de résidence. Elle peut également attester de l'existence d'un document à un moment déterminé.

ou plusieurs utilisateurs de créer et d'attribuer leur clé publique et leur certificat »[228].

1° Leur mission première est la certification des clés publiques et donc l'émission de certificats de clé publique.[229] Lorsqu'elle certifie une clé publique, l'autorité de certification vise à s'assurer de l'identité de la personne à qui appartient la clé publique et ce afin de garantir à toute personne, qui aurait à utiliser telle clé publique déterminée qu'à cette clé publique correspond bien tel individu.

Suite à cette certification, l'autorité de certification émet un certificat de clé publique. Ce certificat est une constatation signée électroniquement émanant d'une autorité de certification, relative à l'identité du sujet mentionné dans le certificat de clé publique et à la clé publique correspondante.

En plus de ces informations factuelles, le certificat peut également contenir ou faire référence aux conditions juridiques en rapport avec ce certificat. De telles conditions sont relatives aux conditions dans lesquelles le certificat a été émis et au statut juridique de l'autorité de certification.

Pour le destinataire d'un certificat, il faut qu'apparaisse clairement la signification du certificat et l'étendue de la confiance qu'on peut y placer. Par exemple, il convient de préciser les conditions de l'émission du certificat et le degré d'exactitude des affirmations contenues dans le certificat. Pour l'autorité de certification, ces conditions juridiques sont de première importance en vue de limiter ou d'exclure, dans une certaine mesure, sa responsabilité, dans le respect des tiers, tel le destinataire du certificat. De l'autre coté, le destinataire peut rechercher à engager la responsabilité de l'autorité de certification pour le respect des termes spécifiés.

2° L'autorité de certification doit veiller à la constitution et à l'actualisation du répertoire contenant les certificats de clé publique qu'elle a émis. Elle aura en charge la suspension et la révocation des certificats. L'autorité devra également intervenir pour assurer l'expiration, la réinscription et le renouvellement des certificats.

228 UIT-T, Recommandation X. 509, Annuaire- cadre d'authentification, note 323, art. 3.3 c).

229 Dans une architecture à clé publique, « l'utilisation de la clé publique permet de vérifier une signature numérique réalisée à l'aide de la clé secrète correspondante. Néanmoins, il importe de s'assurer que ces clés correspondent bel et bien à l'identité avérée du signataire. Il est en effet possible d'imaginer qu'une personne utilise une paire de clés asymétriques en présentant frauduleusement celles-ci comme correspondant à l'identité d'un tiers ou d'une personne fictive; l'utilisation de certificats, émis par une autorité de certification, permet de pallier à cette difficulté ». S. PARISIEN, P. TRUDEL, *op. cit.*, pp. 157-158.

IV.2.3. Le niveau de sécurité et la régénération des clés

IV.2.3.1. Choix d'un niveau de sécurité adéquat

La sécurité totale n'existe pas. En cryptographie, la sécurité d'une clé s'évalue en considération du temps et de l'argent nécessaire à un fraudeur pour casser cette clé. La clé sera réputée sûre si le bénéfice que le fraudeur pourrait tirer du décryptage est minime en fonction des efforts à fournir.

Apparaît ainsi l'idée qu'il peut y avoir des exigences variables quant à la qualité des signatures, en particulier selon l'importance du message.[230]

Ainsi, lorsqu'un contractant souhaite sécuriser ses transactions, il doit déterminer l'enjeu financier des opérations, afin de choisir le niveau de sécurité adéquat. Dans le système Belsign, le client a le choix entre trois niveaux de sécurité distincts[231]. Une sécurité relativement limitée pouvant parfaitement convenir pour des opérations de moindre importance. En fonction des différents niveaux de certificats, les contrôles, les garanties et responsabilités de l'Autorité de Certification varieront.

IV.2.3.2. L'obsolescence des clés et signatures

Une clé réputée indéchiffrable à ce jour pourrait ne plus l'être dans 15 ou 20 ans. Quelle valeur pourra-t-on reconnaître alors aux éléments de preuve constitués aujourd'hui ? Les solutions préconisées par les projets allemands[232] semblent parfaitement adaptées. La durée de sécurité d'une signature électronique est limitée à 5 ans et pour conserver sa valeur probante le document devra être resigné avant l'expiration de cette période de 5 ans[233].

IV.2.4. Les responsabilités de l'autorité de certification

On l'aura compris, les missions des autorités de certification sont capitales. Entre leurs mains résident la sécurisation des réseaux et par là même le développement d'Internet à des fins commerciales.

Le premier champ de responsabilité de l'autorité de certification réside dans l'émission du certificat. « En émettant un certificat, l'autorité de

230 Y. POULLET, *op. cit.*, p. 13; M. FROOMKIN, *op. cit.*, p. 5. Ce dernier envisage les différents niveaux de signature en fonction de la nature de l'opération, en référence à ce qu'offre l'autorité de certification VeriSign.

231 http://www.belsign.be.

232 German Draft Digital Signature Law, disponible en anglais à l'adresse http://ourworld.compuserve.com/homepage/ckuner/digsig.htm#German Digital Signature Law
German Draft Digital Signature Ordinance, disponible en anglais à l'adresse http://ourworld.compuserve.com/homepage/ckuner/verord.htm#German Draft Digital Signature Ordinanc

233 §18 du German Draft Digital Signature Ordinance, *loc. cit.*

certification confirme que les informations qui y figurent sont exactes et complètes »[234]. L'utilisateur est en droit de s'attendre à un haut niveau de fiabilité. A défaut de pouvoir offrir une garantie absolue d'exactitude, l'autorité de certification doit indiquer le niveau de garantie qui se rattache au certificat.

L'autorité de certification pourra être tenue pour responsable d'un manquement à l'obligation de sécurité, particulièrement lorsque la confidentialité de sa propre clé secrète est compromise[235].

« La responsabilité d'une autorité de certification peut également être engagée si celle-ci ne procède pas, de façon diligente, à la suspension ou à la révocation de certificats, ainsi qu'à la publication des certificats ainsi invalidés »[236].

IV.3. La réception en droit de la signature électronique

Il convient de signaler que nous avons à traiter dans ce chapitre de deux problèmes distincts : d'une part, définir ce qu'il faut entendre par une signature électronique, d'autre part, reconnaître une valeur en droit à cette signature.

IV.3.1. Il convient de définir les mécanismes de signature électronique

Différentes législations offrent aujourd'hui une définition de la signature électronique. La plus célèbre et la première est le Digital Signature Act de l'Etat de l'Utah[237]. Dans ce texte, le choix s'est porté sur les mécanismes de signature issus des techniques de cryptographie asymétrique.

Certains auteurs reprochent à ce texte de ne pas disposer de la souplesse nécessaire pour répondre aux changements rapides et incessants du commerce électronique[238]. Effectivement, nous sommes en matière de signature dans une zone de turbulence, la belle stabilité affichée par la signature manuscrite n'est plus de mise. Il faut avoir à l'esprit les progrès techniques futurs dans la définition des exigences de signatures.

234 S. PARISIEN, P. TRUDEL, *op. cit.*, p. 182-183.

235 S. PARISIEN, P. TRUDEL, *op. cit.*, p. 182.

236 S. PARISIEN, P. TRUDEL, *op. cit.*, p. 182.

237 Ce texte a été publié intégralement dans l'EDI Law Review, 1995, 2, 157-196.

238 S. PARISIEN, « Un essai sur le mode de formation des normes dans le commerce électronique », Cybernews, Vol II No II, 1996, pp. 1-2, disponible à l'adresse http://www.droit.umontral.ca/CRDP/CyberNews.

A cet égard, la définition de la signature électronique retenue dans le projet de loi allemand est assez séduisante : elle intègre l'ensemble des fonctionnalités spécifiques à la signature électronique[239].

Enfin, il faut souligner la nécessité d'une normalisation : l'adoption à grande échelle de la signature exigera un consensus sur les standards, de même que l'identification du rôle et des responsabilités de toutes les entités impliquées dans l'utilisation de la signature électronique.

IV.3.2. Il convient d'adapter le système juridique en vue de la réception des mécanismes de signature électronique préalablement définis

Dans l'immédiat, c'est bien les exigences en matière de preuve qui posent problème. On doit se poser la question de l'adéquation des dispositions relatives à la preuve. On aurait tout à gagner en précisant les conditions de recevabilité des preuves électroniques. Dès lors, on peut plaider pour une disposition nouvelle assimilant à une signature manuscrite des signatures électroniques répondant à certains standards.

Un autre aspect de la réflexion consiste à resituer la signature dans le débat juridique. Il faut rendre compte du rôle capital de la signature électronique, à savoir la sécurisation de la communication électronique en vue d'échanges contraignants.

239 German Draft Digital Signature Law, §2, disponible en anglais à l'adresse http://ourworld.compuserve.com/homepage/ckuner/digsig.htm#German Digital Signature Law.